

# Entanglement and Designs

Matthew A. Graydon<sup>1,2,3,\*</sup> and D. M. Appleby<sup>4,†</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, 31 Caroline St. N., Waterloo, Ontario N2L 2Y5, Canada*

<sup>2</sup>*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

<sup>3</sup>*Department of Physics & Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

<sup>4</sup>*Centre for Engineered Quantum Systems, School of Physics,  
The University of Sydney, Sydney, NSW 2006, Australia*

(Dated: September 6, 2016)

We describe a connection between entanglement and designs. It involves the conical 2-designs introduced in a previous paper. These are a generalization of projective 2-designs which includes full sets of arbitrary rank mutually unbiased measurements (MUMs) and arbitrary rank symmetric informationally complete measurements (SIMs), as well as the more familiar MUBs and SICs. We show that a POVM is a conical 2-design if and only if there exists what we call a regular entanglement monotone whose restriction to the pure states is a function of the norm of the probability vector. In that case the concurrence is such a monotone. We also generalize and develop previous work on designs and entanglement detection.

PACS numbers: 03.65.Ud, 03.67.Mn, 03.65.Ta

## I. INTRODUCTION

Entanglement is fundamental in quantum physics. Complex projective 2-designs—geometric structures such as full sets of MUBs (mutually unbiased bases) [1–4] and SICs (symmetric informationally complete measurements of unit rank) [5–7]—are also important. Recently some connections have been found between the two areas [8–14]. We describe a quite different connection.

The connection involves the concurrence [15–17]. This is an entanglement monotone [18] which is simply related to the entanglement of formation [19] and which has some useful properties. Computing entanglement monotones for an arbitrary mixed state can be a difficult problem. The concurrence has the useful feature that it has easily computable lower and upper bounds [20, 21]. In the case of a pair of qubits there is an explicit formula for the concurrence itself [15]. Another useful property is the fact that it vanishes if and only if the state is separable. Finally, it illuminates the monogamous character of entanglement [22].

The connection also involves conical designs [23]. A complex projective 2-design [5, 24–26] is a set of pure states  $\Pi_1, \dots, \Pi_m$  such that  $\sum_{\alpha} \Pi_{\alpha} \otimes \Pi_{\alpha}$  is proportional to the projector onto the symmetric subspace of  $\mathcal{H} \otimes \mathcal{H}$  (where  $\mathcal{H}$  is a fixed  $d$  dimensional complex Hilbert space). A conical 2-design is a generalization in which the rank 1 and trace 1 conditions are relaxed. Specifically it is a set of positive semi-definite operators  $E_1, \dots, E_m$  such that

$$\sum_{\alpha} E_{\alpha} \otimes E_{\alpha} = k_s \Pi_{\text{sym}} + k_a \Pi_{\text{asym}}, \quad k_s > k_a \geq 0 \quad (1)$$

where  $\Pi_{\text{sym}}$  and  $\Pi_{\text{asym}}$  are respectively the projectors onto the symmetric and anti-symmetric subspaces of  $\mathcal{H} \otimes \mathcal{H}$ . It can be shown that  $k_a = 0$  if and only if  $E_{\alpha}$  are all rank 1, in which case they form a weighted complex projective 2-design (up to scaling). Full sets of arbitrary

rank mutually unbiased measurements (MUMs) [27] and arbitrary rank symmetric informationally complete measurements (SIMs) [28] are conical 2-designs.

We will need the following topological concept. Let  $\mathcal{S}$  be the unit sphere in  $\mathcal{H} \otimes \mathcal{H}$ . We say that an entanglement monotone  $M$  is regular if for all  $x$  the set  $\{|\Psi\rangle \in \mathcal{S} : M(|\Psi\rangle) = x\}$  has empty interior (i.e. every point in the set is the limit of a sequence of points outside it [29]). Observe that if  $\{|\Psi\rangle \in \mathcal{S} : M(|\Psi\rangle) = x\}$  has  $\mu$ -measure zero for all  $x$ , then the monotone is regular ( $\mu$  being the usual invariant measure on  $\mathcal{S}$ ). The condition is satisfied by a wide variety of monotones. In particular, the concurrence is regular.

We are now ready to state our main result. Let  $E_{\alpha}$  be an arbitrary POVM on  $\mathcal{H}$ . Let  $|\Psi\rangle \in \mathcal{S}$ ,

$$p_{\alpha,\beta} = \langle \Psi | E_{\alpha} \otimes E_{\beta} | \Psi \rangle \quad (2)$$

be the outcome probabilities for the bipartite product measurement  $E_{\alpha} \otimes E_{\beta}$ ,

$$\|\vec{p}\| = \sqrt{\sum_{\alpha,\beta} p_{\alpha,\beta}^2} \quad (3)$$

be the norm of the probability vector, and  $C(|\Psi\rangle)$  be the concurrence.

**Theorem 1.**  $E_{\alpha}$  is a conical 2-design if and only if there exists a regular entanglement monotone whose restriction to  $\mathcal{S}$  is a function of  $\|\vec{p}\|$ . In that case the restriction of the concurrence is a function of  $\|\vec{p}\|$ . Specifically

$$C(|\Psi\rangle) = 2\sqrt{\frac{k_s^2 - \|\vec{p}\|^2}{k_s^2 - k_a^2}}. \quad (4)$$

Given that  $C(|\Psi\rangle)^2$  is necessarily quadratic in the probabilities it seems fair to say that Eq. (4) is about

the simplest expression conceivable. A simple description of entanglement in terms of probabilities is important in those theoretical approaches which seek to formulate quantum mechanics in purely probabilistic language [30–32]. The simplicity of the result—the fact that conical designs are naturally adapted to the description of entanglement—means that it is likely to be important for other reasons also.

It may be possible to strengthen theorem 1, so that it states that  $E_\alpha$  is a conical 2-design if and only if there is any monotone at all whose restriction to  $\mathcal{S}$  is a function of  $\|\vec{p}\|$ . However, we have not been able to prove it.

The next three sections are devoted to the proof of theorem 1. In Section V we generalize the results of refs. [9–11] to the case of an arbitrary conical 2-design, and compare them to the result just described.

## II. THEOREM 1: NECESSITY

Let  $E_\alpha$  be a POVM which is also a conical 2-design, and let  $|\Psi\rangle \in \mathcal{S}$  have Schmidt decomposition

$$|\Psi\rangle = \sum_r \lambda_r (|f_r\rangle \otimes |g_r\rangle), \quad \sum_r \lambda_r^2 = 1, \quad \lambda_r \geq 0 \quad (5)$$

where  $|f_r\rangle, |g_r\rangle$  are ONBs. Then Eq. (1) implies

$$\begin{aligned} \|\vec{p}\|^2 &= \sum_{\alpha, \beta} \langle \Psi | E_\alpha \otimes E_\beta | \Psi \rangle^2 \\ &= \langle \Psi | \otimes \langle \Psi | \sum_{\alpha, \beta} (E_\alpha \otimes E_\beta) \otimes (E_\alpha \otimes E_\beta) | \Psi \rangle \otimes | \Psi \rangle \\ &= \sum_{r, s, u, v} \lambda_r \lambda_s \lambda_u \lambda_v \left( \frac{k_+ \delta_{rs} \delta_{uv}}{2} + \frac{k_- \delta_{ru} \delta_{sv}}{2} \right)^2 \\ &= \frac{k_s^2 + k_a^2}{2} + \frac{k_s^2 - k_a^2}{2} \sum_{r=1}^d \lambda_r^4 \end{aligned} \quad (6)$$

where  $k_\pm = k_s \pm k_a$ . Consequently [16] (with  $\rho$  being the reduced density matrix of either of the two subsystems)

$$C(|\Psi\rangle) = \sqrt{2 - 2\text{Tr}(\rho^2)} = 2\sqrt{\frac{k_s^2 - \|\vec{p}\|^2}{k_s^2 - k_a^2}} \quad (7)$$

## III. LOCAL UNITARY INVARIANCE

In this section we prove a subsidiary result which is needed to complete the proof of theorem 1. Define a non-trivial local unitary invariant to be a function  $f$  on  $\mathcal{S}$  which is (a) not constant and (b) such that  $f(U \otimes V |\Psi\rangle) = f(|\Psi\rangle)$  for all  $|\Psi\rangle$  and  $U, V \in \text{U}(d)$  (where  $\text{U}(d)$  is the unitary group in dimension  $d$ ).

**Lemma 2.**  $E_\alpha$  is a conical 2-design if and only if  $\|\vec{p}\|$  is a non-trivial local unitary invariant.

*Proof.* Necessity is an immediate consequence of Eq. (6) together with the fact that  $k_s > k_a$ . To prove sufficiency,

let  $E_\alpha$  be a POVM such that  $\|\vec{p}\|$  is a non-trivial local unitary invariant. Define, for all  $U \in \text{U}(d)$ ,

$$E_\alpha^U = U^\dagger E_\alpha U, \quad N^U = \sum_\alpha E_\alpha^U \otimes E_\alpha^U. \quad (8)$$

We will show that  $N^U$  is independent of  $U$ .

Let  $W_{23}$  be the unitary operator which swaps the second and third factors in  $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ . Local unitary invariance means

$$\|\vec{p}\|^2 = \langle \Psi | \otimes \langle \Psi | W_{23} (N^U \otimes N^V) W_{23} | \Psi \rangle \otimes | \Psi \rangle \quad (9)$$

is independent of  $U, V$  for all  $|\Psi\rangle$ . Note that this remains true even if  $|\Psi\rangle$  is not normalized (although  $\vec{p}$  then loses its interpretation as a probability vector).

Let  $|\psi_0\rangle, |\psi_1\rangle$  be arbitrary vectors in  $\mathcal{H}$  and  $e^{i\theta}$  an arbitrary phase. Define

$$|\Psi\rangle = \sum_{n=0}^1 e^{ni\theta} |\psi_n\rangle \otimes |\psi_n\rangle. \quad (10)$$

Then

$$W_{23} (|\Psi\rangle \otimes |\Psi\rangle) = \sum_{n=0}^2 e^{in\theta} |\Xi_n\rangle \quad (11)$$

where we have defined  $|\Xi_0\rangle = |\psi_0\rangle \otimes |\psi_0\rangle \otimes |\psi_0\rangle \otimes |\psi_0\rangle$ ,  $|\Xi_1\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_0\rangle \otimes |\psi_1\rangle + |\psi_1\rangle \otimes |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_0\rangle$ , and  $|\Xi_2\rangle = |\psi_1\rangle \otimes |\psi_1\rangle \otimes |\psi_1\rangle \otimes |\psi_1\rangle$ . Substituting into Eq. (9) gives

$$\|\vec{p}\|^2 = \sum_{n=-2}^2 A_n(U, V) e^{in\theta} \quad (12)$$

where

$$A_n(U, V) = \sum_{r, s=0}^2 \delta_{s, r+n} \langle \Xi_r | N^U \otimes N^V | \Xi_s \rangle. \quad (13)$$

The arbitrariness of  $e^{i\theta}$  means that the coefficients in this expansion are independent of  $U, V$ . In particular

$$A_0(U, V) = \sum_{n=0}^2 \langle \Xi_n | N^U \otimes N^V | \Xi_n \rangle \quad (14)$$

is independent of  $U, V$ . Setting  $|\psi_1\rangle = 0$  (respectively,  $|\psi_0\rangle = 0$ ) in Eq. (14) shows that the  $n = 0$  (respectively,  $n = 2$ ) term on the right hand side is independent of  $U, V$ . So all three terms are independent of  $U, V$ . Now observe that  $N^U$  commutes with  $W_{12}$ , the unitary operator which swaps the two factors in  $\mathcal{H} \otimes \mathcal{H}$ . It follows that, if we define

$$\vec{L}^U = \left( \langle \psi_0 | \otimes \langle \psi_1 | N^U | \psi_0 \rangle \otimes | \psi_1 \rangle \right), \quad (15)$$

then  $\vec{L}^U \cdot \vec{L}^V$  is independent of  $U, V$ . So

$$\vec{L}^U \cdot \vec{L}^U = \vec{L}^V \cdot \vec{L}^V = \vec{L}^U \cdot \vec{L}^V. \quad (16)$$

for all  $U, V$ . Since the components of  $\vec{L}^U, \vec{L}^V$  are real, non-negative this means  $\vec{L}^U = \vec{L}^V$ . In particular

$$\langle \psi_0 | \otimes \langle \psi_1 | N^U | \psi_0 \rangle \otimes | \psi_1 \rangle \quad (17)$$

is independent of  $U$ .

Now let  $|\phi_0\rangle, |\phi_1\rangle, |\chi_1\rangle, |\chi_2\rangle$  be arbitrary vectors in  $\mathcal{H}$  and  $e^{i\theta}$  an arbitrary phase. Define

$$|\psi_0\rangle = \sum_{n=0}^1 e^{in\theta} |\phi_n\rangle \quad |\psi_1\rangle = \sum_{n=0}^1 e^{2in\theta} |\chi_n\rangle \quad (18)$$

Then

$$\langle \psi_0 | \otimes \langle \psi_1 | N^U | \psi_0 \rangle \otimes | \psi_1 \rangle = \sum_{n=-3}^3 B_n(U) e^{in\theta} \quad (19)$$

where

$$B_n(U) = \sum_{\substack{r_2+2s_2= \\ r_1+2s_1+n}} \langle \phi_{r_1} | \otimes \langle \chi_{s_1} | N^U | \phi_{r_2} \rangle \otimes | \chi_{s_2} \rangle \quad (20)$$

The arbitrariness of  $e^{i\theta}$  means that the individual coefficients in this expansion must be independent of  $U$ . In particular

$$B_3(U) = \langle \phi_0 | \otimes \langle \chi_0 | N^U | \phi_1 \rangle \otimes | \chi_1 \rangle \quad (21)$$

is independent of  $U$ . Since the product states span  $\mathcal{H} \otimes \mathcal{H}$  this means  $N^U$  is independent of  $U$ . In other words  $\sum_{\alpha} E_{\alpha} \otimes E_{\alpha}$  commutes with  $U \otimes U$  for all  $U$ . Theorem 1 in ref. [23] then implies

$$\sum_{\alpha} E_{\alpha} \otimes E_{\alpha} = k_s \Pi_{\text{sym}} + k_a \Pi_{\text{asym}} \quad (22)$$

for some  $k_s \geq k_a \geq 0$ . If  $k_s = k_a$  then  $\sum_{\alpha} E_{\alpha} \otimes E_{\alpha} = k_s I$ , implying  $\|\vec{p}\| = k_s$  for all  $\|\vec{p}\|$ , contradicting the fact that  $\|\vec{p}\|$  is a non-trivial invariant. So  $k_s > k_a$  and  $E_{\alpha}$  is a conical 2-design.  $\square$

#### IV. THEOREM 1: SUFFICIENCY

Suppose  $M$  is a regular entanglement monotone such that  $M = f(\|\vec{p}\|)$  on  $\mathcal{S}$ , for some function  $f$ . We first show that  $\|\vec{p}\|$  must be a non-trivial local unitary invariant. For suppose that were not the case. Then either  $\|\vec{p}\|$  would be trivial or else it would not be a local unitary invariant. The first possibility would imply that  $M$  was constant on  $\mathcal{S}$ , contradicting the fact that  $M$  is assumed regular. The second possibility would imply that, for some fixed  $|\Psi\rangle$ , the map

$$(U, V) \in \text{U}(d) \times \text{U}(d) \rightarrow \sqrt{\langle \Psi | \otimes \langle \Psi | W_{23} (N^U \otimes N^V) W_{23} | \Psi \rangle \otimes | \Psi \rangle} \in \mathbb{R} \quad (23)$$

took at least two distinct values, say  $a < b$ . The continuity of the map together with the connectedness of the group  $\text{U}(d) \times \text{U}(d)$  would then imply that it took every value in the interval  $[a, b]$ . On the other hand, the restriction of  $M$  to  $\mathcal{S}$  is a local unitary invariant [18]. So  $f$  would have to take the same constant value, call it  $x$ , for every element of  $[a, b]$ . This would mean that  $\{|\Psi\rangle \in \mathcal{S} : M(|\Psi\rangle) = x\}$  contained the non-empty open set  $\{|\Psi\rangle \in \mathcal{S} : a < \|\vec{p}\| < b\}$ , again contradicting the fact that  $M$  is assumed regular. It now follows from Lemma 2 that  $E_{\alpha}$  is a conical 2-design.

#### V. WITNESSES

Having established our main result we now compare it with the results in refs. [9–13]. We begin with refs. [9–12]. Although the authors do not present it this way what is done in these papers is, in effect, to show that there is a natural way to construct entanglement witnesses out of MUMs and SIMs (as noted in ref. [33]). Let  $\mathcal{S}_s$  be the subset of  $\mathcal{S}$  consisting of the separable pure states. Given an arbitrary Hermitian operator  $A$  on  $\mathcal{H} \otimes \mathcal{H}$  define

$$s_A^- = \inf_{|\Psi\rangle \in \mathcal{S}_s} \{\langle \Psi | A | \Psi \rangle\} \quad s_A^+ = \sup_{|\Psi\rangle \in \mathcal{S}_s} \{\langle \Psi | A | \Psi \rangle\} \quad (24)$$

$$e_A^- = \inf_{|\Psi\rangle \in \mathcal{S}} \{\langle \Psi | A | \Psi \rangle\} \quad e_A^+ = \sup_{|\Psi\rangle \in \mathcal{S}} \{\langle \Psi | A | \Psi \rangle\} \quad (25)$$

Then  $s_A^+ I - A$  (respectively  $A - s_A^- I$ ) is an entanglement witness [33, 34] if and only if  $e_A^+ > s_A^+$  (respectively  $e_A^- < s_A^-$ ), in which case we will say  $A$  detects entanglement from above (respectively below). If, on the other hand,  $s_A^{\pm} = e_A^{\pm}$ , then a measurement of  $A$  cannot detect entanglement. In refs. [9–11] the authors only consider detection from above, although detection from below is also possible, as we will see.

Let  $E_{\alpha}$  be an arbitrary conical 2-design and let  $|e_j\rangle$  be some fixed ONB in  $\mathcal{H}$ . Define

$$N = \sum_{\alpha} E_{\alpha} \otimes E_{\alpha}, \quad N^{\text{PT}} = \sum_{\alpha} E_{\alpha} \otimes E_{\alpha}^{\text{T}}, \quad (26)$$

where  $N^{\text{PT}}$  (respectively  $E_{\alpha}^{\text{T}}$ ) is the partial transpose (respectively transpose) of  $N$  (respectively  $E_{\alpha}$ ) relative to the basis  $|e_j\rangle$ . It follows from Eq. (1) in this paper and Theorem 1 in ref. [23] that

$$N = k_+ I + k_- W_{12}, \quad N^{\text{PT}} = k_+ I + dk_- |\Phi_+\rangle \langle \Phi_+|, \quad (27)$$

where  $k_{\pm} = (k_s \pm k_a)/2$ ,  $W_{12}$  is the unitary which swaps the two factors in  $\mathcal{H} \otimes \mathcal{H}$ , and  $|\Phi_+\rangle$  is the maximally entangled state  $(1/\sqrt{d}) \sum_j |e_j\rangle \otimes |e_j\rangle$ . One easily sees

$$s_N^- = k_+, \quad s_N^+ = k_+ + k_-, \quad (28)$$

$$e_N^- = k_+ - k_-, \quad e_N^+ = k_+ + k_-. \quad (29)$$

So  $N$  can detect entanglement from below, but not from above. On the other hand

$$s_{N^{\text{PT}}}^- = k_+, \quad s_{N^{\text{PT}}}^+ = k_+ + k_-, \quad (30)$$

$$e_{N^{\text{PT}}}^- = k_+, \quad e_{N^{\text{PT}}}^+ = k_+ + dk_-. \quad (31)$$

So  $N^{\text{PT}}$  can detect entanglement from above, but not from below. Let us note that in refs. [9–12] the authors calculate  $c_+^s(N)$  for MUMs and SIMs, but not  $c_+(N)$ . Consequently, they do not draw the conclusion, that  $N$  cannot detect entanglement from above.

In refs. [9–12] the authors also consider operators of the more general form

$$N_{\text{gen}} = \sum_{\alpha} E_{\alpha} \otimes F_{\alpha} \quad (32)$$

where  $E_{\alpha}, F_{\alpha}$  are distinct MUMs or SIMs. Calculating  $c_{\pm}^s(N_{\text{gen}})$ ,  $c_{\pm}(N_{\text{gen}})$  for arbitrary pairs of conical designs is beyond our present scope. In this connection let us note that the authors of refs. [9–12] do not calculate them either (although refs. [9–11] do calculate a bound for  $c_+^s(N_{\text{gen}})$  valid for pairs of MUMs or SIMs having the same contraction parameter [23], extended in ref. [12] to pairs of MUMs having different contraction parameters).

Liu *et al* [12] consider the application of MUMs to multipartite entanglement. However, they do not show that their bound is violated for any non-separable states.

Shen *et al* [13] consider detection criteria which are non-linear in the density matrix. It is easily seen that their criteria generalize to the statements that, for any conical design, and any separable density matrix  $\rho$ , the quantities  $|\text{Tr}(N(\rho - \rho_1 \otimes \rho_2))|$ ,  $|\text{Tr}(N^{\text{PT}}(\rho - \rho_1 \otimes \rho_2))|$  are both bounded above by  $k_- \sqrt{(1 - \text{Tr}(\rho_1^2))(1 - \text{Tr}(\rho_2^2))}$ , where  $\rho_j$  is the reduced density matrix for the  $j^{\text{th}}$  subsystem. It is easily verified that every entangled state detected by the criterion  $\text{Tr}(\rho N^{\text{PT}}) > s_{N^{\text{PT}}}^+$  is also detected by the corresponding quadratic criterion. On the other hand there exist states which are detected by the criterion  $\text{Tr}(\rho N) < s_N^-$  but which are not detected by the corresponding quadratic criterion. Consider, for instance, the entangled Werner state [35]

$$\rho_W = \frac{2(1-p)}{d(d+1)} \Pi_{\text{sym}} + \frac{2p}{d(d-1)} \Pi_{\text{asym}} \quad \frac{1}{2} < p \leq 1 \quad (33)$$

The linear criterion involving  $N$  detects the entanglement for all values of  $p$  whereas the quadratic criterion only detects it for  $p > (d-1)/d$ . This does not conflict with Shen *et al*'s analysis because they do not consider the possibility of detection from below.

The witnesses corresponding to  $N$  and  $N^{\text{PT}}$  are

$$N - s_N^- I = k_- W_{12} \quad (34)$$

$$s_{N^{\text{PT}}}^+ I - N^{\text{PT}} = k_- (I - d|\Phi_+\rangle\langle\Phi_+|) \quad (35)$$

The fact that these are witnesses is, of course, well known (see, e.g., Example 3.1 in ref. [33]; Eq. (28) in ref. [34]). The novelty of refs. [9–12] is that they show that the witnesses have simple expressions in terms of the probabilities obtained from local measurements. The simplicity of the expressions means they have an obvious theoretical interest. Their experimental interest is less obvious, since obtaining the probabilities empirically amounts to performing full-state tomography; and once one has done that one can calculate any witness one wants. It is to be observed, however, that one may be able to truncate the design and still have an entanglement witness (as is shown in Appendix A of Spengler *et al* [9] for MUBs). As Spengler *et al* note this may be experimentally useful, especially when  $d$  is large.

To summarize, we have shown that a well-known entanglement monotone has a simple expression in terms of design probabilities while refs. [9–11] have done the same for two well-known entanglement witnesses. The crucial difference is that theorem 1 gives a condition which is both necessary and sufficient for a given POVM to be a conical 2-design, whereas continuity means that the inequalities  $s_N^- > e_N^-$ ,  $s_{N^{\text{PT}}}^+ < e_{N^{\text{PT}}}^+$  will remain valid even after the  $E_{\alpha}$  have been significantly and randomly perturbed. Consequently, the inequalities proved in refs. [9–13] can detect entanglement for a wide variety of POVMs which are not conical 2-designs. In that sense the connection we exhibit, between designs and entanglement, is tighter than the one exhibited in refs. [9–13].

## CONCLUSION

We showed that a POVM is a conical 2-design if and only if there is a regular entanglement monotone which is a function of  $\|\vec{p}\|$ . We went on to extend the results in refs. [9–13], and to compare them with our theorem 1. In particular we showed that there is a natural way to construct entanglement witnesses out of an arbitrary conical design. However, the connection between witnesses and designs is less tight than the one between monotones and designs, in the sense explained in the last section. Our work naturally suggests the question, whether there are similar connections between multipartite entanglement and conical  $t$ -designs with  $t > 2$ .

## ACKNOWLEDGEMENTS

We gratefully acknowledge Chris Fuchs for stimulating discussions. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research & Innovation. MAG was supported by an NSERC Alexander Graham Bell Canada Graduate Scholarship. DMA was supported by the IARPA MQCO program, by the ARC via EQuS project number CE11001013, and by the US Army Research Office grant numbers W911NF-14-1-0098 and W911NF-14-1-0103.

---

\* mgraydon[at]perimeterinstitute.ca

† marcus[at]physics.usyd.edu

- [1] J. Schwinger, Proc. Natl. Acad. Sci. USA **46**, 570 (1960).
- [2] I. D. Ivanovic, J. Phys. A: Math. Gen. **14**, 3241 (1981).
- [3] W. K. Wootters and B. D. Fields, Ann. Phys. **81**, 363 (1989).
- [4] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum Inf. **8**, 535 (2010).
- [5] G. Zauner, *Quantendesigns, Grundzüge einer nichtkommutativen Designtheorie (in German)*, Ph.D. thesis, University of Vienna (1999), English translation: G. Zauner, Int. J. Quantum Inf. **9**, 445 (2011)].
- [6] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
- [7] A. J. Scott and M. Grassl, Journal of Mathematical Physics **51**, 042203 (2010).
- [8] M. Wieśniak, T. Paterek, and A. Zeilinger, New J. Phys. **13**, 053047 (2011).
- [9] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Phys. Rev. A **83**, 022311 (2012).
- [10] B. Chen, T. Ma, and S.-M. Fei, Phys. Rev. A **89**, 064302 (2014).
- [11] B. Chen, T. Li, and S.-M. Fei, Quantum Information Processing **14**, 2281 (2015).
- [12] L. Liu, T. Gao, and F. Yan, Scientific Reports **5**, 13138 (2015).
- [13] S.-Q. Shen, M. Li, and X.-F. Duan, Phys. Rev. A **91**, 012326 (2015).
- [14] A. Kalev and J. Bae, Phys. Rev. A **87**, 062314 (2013).
- [15] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
- [16] P. Rungta, V. Buzek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).
- [17] P. Rungta and C. M. Caves, Phys. Rev. A **67**, 012307 (2003).
- [18] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [19] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [20] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 16790 (2004).
- [21] F. Mintert, *Measures and dynamics of entangled states*, Ph.D. thesis, LMU München (2004).
- [22] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
- [23] M. A. Graydon and D. M. Appleby, J. Phys. A: Math. Theor. **49**, 085301 (2016).
- [24] A. Neumaier, “Combinatorial configurations in terms of distances,” Depart. of Mathematics Memorandum 81-09, Eindhoven University of Technology (1981).
- [25] S. G. Hoggar, Europ. J. Combin. **69**, 2881 (1982).
- [26] A. J. Scott, J. Phys. A: Math. Gen. **39**, 13507 (2006).
- [27] A. Kalev and G. Gour, New J. Phys. **16**, 053038 (2014).
- [28] D. M. Appleby, Optics and Spectroscopy **103**, 416 (2007).
- [29] J. Dugundji, *Topology* (Allyn and Bacon, 1966).
- [30] C. A. Fuchs, arXiv:1003.5209 [quant-ph] (2010).
- [31] C. A. Fuchs and R. Schack, Rev. Mod. Phys. **85**, 1693 (2013).
- [32] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, in *Mathematical Foundations of Information Flow*, edited by S. Abramsky and M. Mislove (Proc. of Symposia in Applied Mathematics, 2012) pp. 25–47.
- [33] D. Chruściński and G. Sarbicki, J. Phys. A: Math. Theor. **47**, 483001 (2014).
- [34] O. Gühne and G. Tóth, Physics Reports **474**, 1 (2009).
- [35] R. F. Werner, Physical Review A **40**, 4277 (1989).